



DEPARTMENT OF DEFENSE

Department of the Army

[Docket ID: USA-2021-HQ-0005]

Privacy Act of 1974; System of Records

AGENCY: Department of the Army, Department of Defense (DoD).

ACTION: Notice of a modified system of records.

SUMMARY: The Department of the Army is modifying and renaming the United States Military Entrance Processing Command (USMEPCOM) Integrated Resource System (USMIRS), A0601-270. As the executive agent, the Department of the Army uses the USMIRS to determine the qualifications of applicants for the Armed Forces of the United States through aptitude testing, medical examination, identity verification, background screening, and administrative processing. Records will also be used to determine patterns and trends in the military population, and for statistical analyses.

DATES: This system of records modification is effective upon publication; however, comments on the Routine Uses will be accepted on or before [INSERT 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. The Routine Uses are effective at the close of the comment period.

ADDRESSES: You may submit comments, identified by docket number and title, by any of the following methods:

* Federal Rulemaking Portal: <https://www.regulations.gov>.

Follow the instructions for submitting comments.

* Mail: DoD cannot receive written comments at this time due to the COVID-19 pandemic.

Comments should be sent electronically to the docket listed above.

Instructions: All submissions received must include the agency name and docket number for this *Federal Register* document. The general policy for comments and other submissions from

members of the public is to make these submissions available for public viewing on the Internet at <https://www.regulations.gov> as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: Mr. Myron Wong, Department of the Army, U.S. Army Records Management and Declassification Agency, ATTENTION: Army Privacy and Civil Liberties Office, 9301 Chapek Road (Building 1458), Fort Belvoir, VA 22060-5605, or by calling 571-515-0243.

SUPPLEMENTARY INFORMATION: The USMEPCOM consists of 65 Military Entrance Processing Stations (MEPS) and one Remote Processing Station (RPS) in the United States. The USMIRS conducts aptitude tests, processes medical examinations, and determines acceptability of individuals for entry into the Armed Forces of the United States based on each Service's eligibility standards. The USMIRS also determines acceptability, administratively processes, allocates, and inducts Selective Service System registrants when required; and provides aptitude and medical examination services for other Federal agencies as requested. The USMIRS interfaces with recruiting capabilities for the Services using standard DoD data elements to share data between USMEPCOM and all the Armed Services recruiting and accession commands. Additionally, the USMIRS shares data with the Social Security Administration (SSA) and the United States Citizenship and Immigration Services (USCIS) for identity vetting and to verify eligibility to work in the United States. Applicant information is retained by the USMIRS for various statistical analyses to identify trends and reduce duplicative processes.

This system of records is being modified to alter the system name, modify the system number to remove "DoD" at the end, and to comply with requirements in Office of Management and Budget (OMB) Circular No. A-108 (2016). This modified system of records also expands the purposes of the system of records, the categories of individuals, and the categories of records by, among other things, including language concerning the system's support of Selective Service registration processes and support for other Federal agencies. The modifications include new

and modified routine uses specifying, among other things, the potential sharing of information to authorized representative agents of Federal, state, local, territorial/tribal, international, or foreign agencies for legal, security, health, or other administrative reasons. Changes have also been made to the following sections: system manager; system location; authorities; retrieval of records; procedures for record access and notification, and contesting records; and safeguards.

In addition, the system of records is being modified to reflect major changes to the policies and practices for the retention and disposal of records due to a recent retention schedule change approved by the National Archives and Records Administration (NARA). The change in the system's retention policy was required to support the mobilization requirements in accordance with DoD policy (DoD Instruction 1352.01) and to prevent potential fraudulent enlistments using duplicated Social Security numbers. These changes will require the system to securely retain electronic data in a cloud computing environment to meet business needs prior to being securely archived offsite in a Federal Records Center on encrypted physical storage media.

The DoD notices for systems of records subject to the Privacy Act of 1974, as amended, have been published in the Federal Register and are available from the address in FOR FURTHER INFORMATION CONTACT or at the Defense Privacy, Civil Liberties, and Transparency Division website at <https://dpcl.d.defense.gov>.

In accordance with 5 U.S.C. sec. 552a(r) and OMB Circular No. A-108, the DoD has provided a report of this system of records to the OMB and to Congress.

Dated: April 14, 2021.

Aaron T. Siegel,

Alternate OSD Federal Register

Liaison Officer, Department of Defense.

SYSTEM NAME AND NUMBER: United States Military Entrance Processing Command (USMEPCOM) Integrated Resource System (USMIRS), A0601-270

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Primary location: United States Military Entrance Processing Command (USMEPCOM), 2834 Green Bay Road, North Chicago, IL 60064-3094; digital cloud storage provided by Amazon Web Services (AWS) GovCloud (US), 12900 Worldgate Drive, Building: IAD21, Herndon, VA 20170. Segments exist at Military Entrance Processing Stations (MEPS) throughout the continental United States, Alaska, Hawaii, and Puerto Rico; official mailing addresses are available on the USMEPCOM webpage at <https://www.mepcom.army.mil/MEPS.aspx>.

SYSTEM MANAGER(S): Commander, U.S. Military Entrance Processing Command, 2834 Green Bay Road, North Chicago, IL 60064-3094. Deputy Director, J-6/Information Technology Directorate, (847) 688-3680, ext. 7701.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 10 U.S.C. § 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. Subtitle A, General Military Law, Part II, Personnel (Chapter 31, Enlistments and Chapter 33, Original Appointments of Regular Officers in Grades Above Warrant Officer Grades); 10 U.S.C. § 3013, Secretary of the Army; 10 U.S.C. § 5013, Secretary of the Navy; 10 U.S.C. § 8013, Secretary of the Air Force; DoD Directive (DoDD) 1145.02E, United States Military Entrance Processing Command (USMEPCOM); DoD Instruction (DoDI) 1304.02, Accession Processing Data Collection Forms; DoDI 1304.12E, DoD Military Personnel Accession Testing Programs; DoDI 1304.26, Qualification Standards for Enlistment, Appointment and Induction; DoDI 6130.03, Medical Standards for Appointment, Enlistment, or Induction in the Military Services; DoD Manual 1145.02, Military Entrance Processing Station (MEPS); USMEPCOM Regulation 680-3, Entrance Processing and Reporting System Management; and E.O. 9397 (SSN), as amended.

PURPOSE(S) OF THE SYSTEM: The USMIRS is the official accession system for the Department of Defense (DoD). The USMEPCOM uses it to determine qualifications of applicants for the Armed Forces of the United States through aptitude testing, medical examination, identity verification, background screening, and administrative processing. The USMIRS is also used to determine qualifications for special category, non-enlistment applicants for Selective Service registration, and other Federal agency applicants when required. Accession data for the Services is reported to the Defense Manpower Data Center (DMDC) for applicant processing, reporting requirements, and quality assurance. Records are also used to determine patterns and trends in the military population, support mobilization, prevent fraudulent enlistments, and for statistical analyses.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: All individuals who report to a military entrance test site or MEPS for aptitude testing and/or medical examination to determine their fitness for entry into the U.S. Armed Forces (Army, Navy, Air Force, Marine Corps, and Coast Guard). Individuals may also include Selective Service System inductees and special category non-enlistment applicants from Federal agencies such as the Central Intelligence Agency, Federal Bureau of Investigation, Federal Aviation Administration, and other uniformed services such as the United States Public Health Service Commissioned Corps or the National Oceanic and Atmospheric Administration Commissioned Officer Corps (as required).

CATEGORIES OF RECORDS IN THE SYSTEM: Personally identifying data to include: Full name and other names used; Social Security Number (SSN), DoD Identification (DoD ID) number, alien registration number, selective service registration number; gender; date and place of birth; race and ethnic origin; height, weight, eye color; biometric data (fingerprints and digital photograph); and driver's license number.

Other personal data to include: Marital status; citizenship and immigration status; religious preference, home and mobile telephone number; home and mailing address; state of permanent

residence; personal email address; languages spoken; prior employment; background investigation.

Dependent family member data (emergency contact information) to include: Family members' full names and other names used; date of birth; marital status; home, mobile and work telephone number; and home and work address.

Prior military personnel data to include: Branch; service computation dates; type of discharge; separation reason codes; lost time (absent without leave and desertion); and DoD ID number.

RECORD SOURCE CATEGORIES: The individuals. The individuals' data is also received from records maintained by the DMDC. Information may also be provided by education and financial institutions, law enforcement agencies, the Office of Personnel Management, Social Security Administration, Department of Homeland Security, Department of the Treasury, and other Federal, state and local agencies.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING

CATEGORIES OF USERS AND PURPOSES OF SUCH USES: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, the records contained in this system may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

- a. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government when necessary to accomplish an agency function related to this system of records.
- b. To the appropriate Federal, State, local, territorial, tribal, foreign, or international law enforcement authority or other appropriate entity where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether criminal, civil, or regulatory in nature.

- c. To any component of the Department of Justice for the purpose of representing the DoD, or its components, officers, employees, or members in pending or potential litigation to which the record is pertinent.
- d. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body or official, when the DoD or other Agency representing the DoD determines that the records are relevant and necessary to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.
- e. To the National Archives and Records Administration for the purpose of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.
- f. To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.
- g. To appropriate agencies, entities, and persons when (1) the DoD suspects or confirms a breach of the system of records; (2) the DoD determines as a result of the suspected or confirmed breach there is a risk of harm to individuals, the DoD (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the DoD's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.
- h. To another Federal agency or Federal entity, when the DoD determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

- i. To such recipients and under such circumstances and procedures as are mandated by Federal statute or treaty.
- j. To Federal, State and local health departments for compliance with public health communicable disease reporting laws in accordance with 42 U.S.C. 264.
- k. To the Social Security Administration (SSA) and the United States Citizenship and Immigration Services (USCIS) to verify eligibility to work in the United States as required by 8 U.S.C. 1101 and 8 U.S.C. 1324a.
- l. To the Central Intelligence Agency, Federal Bureau of Investigation, and Federal Aviation Administration; and other uniformed services such as the United States Public Health Service Commissioned Corps or the National Oceanic and Atmospheric Administration Commissioned Officer Corps when medically processing special category non-enlistment applicants on behalf of those agencies.
- m. To the Selective Service System (SSS) to report processing of inductees in support of a military draft, and for the purpose of updating the SSS registrant database as required by 50 U.S.C. 3802.
- n. To other Federal, state, local, territorial or tribal, international, or foreign agencies, and to financial institutions, in order to obtain information relevant and necessary to USMEPCOM's qualification determinations for the individuals covered by this system of records.
- o. To designated officers and employees of Federal, State, local, territorial, tribal, international, or foreign agencies in connection with the hiring or retention of an employee, the conduct of a suitability or security investigation, the letting of a contract, or the issuance of a license, grant or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter and the Department deems appropriate.
- p. To foreign or international law enforcement, security, or investigatory authorities to comply with requirements imposed by, or to claim rights conferred in, international agreements and

arrangements, including those regulating the stationing and status in foreign countries of DoD military and civilian personnel.

q. To appropriate Federal, State, local, territorial, tribal, foreign, or international agencies for the purpose of counterintelligence activities authorized by U.S. law or Executive Order, or for the purpose of executing or enforcing laws designed to protect the national security or homeland security of the United States, including those relating to the sharing of records or information concerning terrorism, homeland security, or law enforcement.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records may be stored electronically or on paper in secure facilities in a locked drawer behind a locked door. Electronic records may be stored locally on digital media; in agency-owned cloud environments; or in vendor Cloud Service Offerings certified under the Federal Risk and Authorization Management Program (FedRAMP).

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records may be retrieved by individual's name, Social Security Number (SSN), DoD Identification Number, USMIRS automatic identification and data capture (AIDC) identification code (barcode), and/or biometric data (fingerprint).

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

All hardcopy applicant records are retained at each MEPS for a period ranging between 2 years, 3 years, or a maximum of 7 years, as defined by individual qualification status, then destroyed. The USMIRS will retain electronic qualified applicant processing records in the system until no longer needed for conducting business. The records will then be placed on physical storage media and transferred to the Federal Records Center (FRC). The FRC will destroy the records when the applicant turns 43 years old. USMIRS will retain electronic permanently disqualified applicant processing records in the system until no longer needed for conducting business. The records will then be placed on physical storage media and transferred to the FRC. The FRC will destroy the records after 99 years.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: Administrative safeguards include periodic security audits, regular monitoring of users' security practices, employment of methods to ensure only authorized personnel have access to personal information, all personnel are required to have appropriate background checks conducted prior to attaining system access, and privileged users are required to attain and maintain certification in accordance with DoD Directive 8140.01 and DoD 8570.01-M. Technical safeguards include user ID and password, intrusion detection system, encryption, external certificate authority, biometrics, firewall, virtual private network, DoD public key infrastructure certificates, common access card, and security technical implementation guides. Physical safeguards include security guards, identification badges, key cards, safes, and cipher locks. All USMIRS servers are stored in either a data center or locked server/communications room.

RECORD ACCESS PROCEDURES: Individuals seeking access to information about themselves contained in this system should address written inquiries to the Commander, U.S. Military Entrance Processing Command, FOIA/PA Officer (J-1/MEHR-PR), 2834 Green Bay Road, North Chicago, IL 60064-3094. Individuals should provide their full name, current address telephone number, and other personal identifying data that would assist in locating the records. In addition, the requester must provide either a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the following format:

If executed outside the United States: "I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on (date). (Signature)."

If executed within the United States, its territories, possessions, or commonwealths: "I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct.

Executed on (date). (Signature)."

CONTESTING RECORD PROCEDURES: The DoD rule for accessing, contesting and appealing agency determinations by the individual concerned are published in 32 CFR part 310 or may be obtained from the system manager.

NOTIFICATION PROCEDURES: Individuals seeking access to information about themselves contained in this system should address written inquiries to the Commander, U.S. Military Entrance Processing Command, FOIA/PA Officer (J-1/MEHR-PR), 2834 Green Bay Road, North Chicago, IL 60064-3094. Individuals should provide their full name, current address telephone number, and other personal identifying data that would assist in locating the records. In addition, the requester must provide either a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the following format:

If executed outside the United States: “I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on (date). (Signature).”

If executed within the United States, its territories, possessions, or commonwealths: “I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct.

Executed on (date). (Signature).”

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: November 3, 2010, 75 FR 67700; February 25, 2005, 70 FR 9284.